

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**  
**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2013 covering the prior calendar year 2012

1. Date filed: February 20, 2013
2. Name of company(s) covered by this certification: Paul Bunyan Rural Telephone Cooperative
3. Form 499 Filer ID: 804129
4. Name of signatory: Elaine Iverson
5. Title of signatory: CPNI Compliance Officer
6. Certification:

I, Elaine Iverson, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed Elaine Iverson 2-20-13

**Attachments:** Accompanying Statement explaining CPNI procedures

## STATEMENT OF COMPLIANCE FOR PAUL BUNYAN RURAL TELEPHONE COOPERATIVE

### **Use of CPNI in Marketing**

Our company does not use CPNI in any of its marketing efforts, and does not permit the use of, or access to, customer CPNI by our affiliates or any third parties. We use, disclose or permit access to CPNI only for the purposes permitted under 47 U.S.C. Sections 222(c)(1) and (d).

### **CPNI Safeguards**

Our company has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.

Our company trains its personnel as to when they are, and are not, authorized to use or disclose CPNI, and we have an express disciplinary process in place if the rules are violated.

Our company authenticates the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or in-store visit.

Our company discloses call detail records (CDR) at the customer's request in person with a valid photo ID or by mailing to the address of record. We do not disclose CDR over the phone.

Our company discloses CPNI to a customer in person at our retail location(s) only when the customer presents a valid photo ID and the ID matches the name on the account.

Our company establishes passwords and security questions with customers in order to authenticate customers. Neither passwords or security questions rely on customers' readily available biographical information.

Our company has established password protection for customers' online accounts.

Our company includes terms specifying the confidentiality and use of CPNI in its contracts with business customers that are served by a dedicated account representative.

Our company notifies a customer of changes in: account number, telephone number, address of record, or online account passwords.

### **CPNI Recordkeeping and Reporting**

Our company is prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. We may also notify the customer of such breach, after consulting with the investigatory agency(ies), if we believe there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. We will notify the customer of the breach after 7 business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.

Our company will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.

Our company is prepared to provide the FCC with written notice, within five business days of any instance where the "opt out" mechanisms to not work properly.